МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ДОНСКОЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
(ДГТУ)
АВИАЦИОННЫЙ КОЛЛЕДЖ

УТВЕРЖДАЮ
Директор колледжа
_____ А.И. Азарова
личная подпись инициалы, фамилия
«___»_____2021г
Рег. № _____

РАБОЧАЯ ПРОГРАММА

По дисциплине _ОП.13 Информационная безопасность_
(шифр дисциплины по учебному плану, название)
По специальности 09.02.07 Информационные системы и программирование
(код, название без кавычек)
Форма и срок освоения ОП: _очная. нормативный_
(очная, заочная, нормативный)

Объем образовательной программы учебной дисциплины ____48__ часов

Из них в семестре:	____2___	_____
Лекции –	____32___ час.	_____ час.
Лабораторные занятия –	_____ час.	_____час.
Практические занятия –	____10__ час.	_____ час
Курсовое проектирование –	_____ час.	_____ час.
Контрольные работы -	_____ час.	_____ час.
Самостоятельная работа	___4____ час.	_____ час.
Промежуточная аттестация	___2____ час.	_____ час.

ФОРМЫ КОНТРОЛЯ

Экзамен ____ семестр
Зачет – _____семестр
Дифференцированный зачет ___2___ семестр
Форма контроля _____семестр

Ростов-на-Дону
2021 г.

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ ОП.13 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

1.1. Место дисциплины в структуре основной профессиональной образовательной программы: Учебная дисциплина «Информационная безопасность» принадлежит к общепрофессиональному циклу.

1.2. Цель и планируемые результаты освоения дисциплины:

Код	Умения	Знания
ОК 01, ОК 02, ОК 05, ОК 09, ОК 10, ПК11.6	применять правовые, организационные, технические и программные средства защиты информации; устный опрос, контроль выполнения практических заданий, контроль самостоятельной работы, тестирование создавать программные средства защиты информации устный опрос, контроль практических работ, заданий, контроль самостоятельной работы	источники возникновения информационных угроз; контроль выполнения практических заданий, устный опрос, контроль самостоятельной работы, тестирование модели и принципы защиты информации от несанкционированного доступа контроль выполнения практических заданий, устный опрос, контроль самостоятельной работы, тестирование методы антивирусной защиты информации контроль выполнения практических заданий, устный опрос, контроль самостоятельной работы, тестирование

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	**Объем в часах**
Объем образовательной программы	**48**
в том числе:	
теоретическое обучение	32
практические занятия	10
Самостоятельная работа	4
Промежуточная аттестация	2

2.2 Тематический план и содержание учебной дисциплины

Наименование разделов и тем	Содержание учебного материала и формы организации деятельности обучающихся	Объем в часах	Коды компетенций, формированию которых способствует элемент программы
1	2	3	4
Раздел 1. Концепция информационной безопасности		**6**	
Тема 1.1 Актуальность информационной безопасности	**Содержание учебного материала**		ОК 01, ОК 02, ОК 05, ОК 09, ОК 10, ПК11.6
	1 Национальные интересы РФ в информационной сфере	2	
Тема 1.2 Лицензирование и сертификация в области защиты информации	**Содержание учебного материала**		
	1 Законодательство в области лицензирования и сертификации	2	
Тема 1.3 Основные нормативные руководящие документы	**Содержание учебного материала**		
	1 Информационные стандарты информационного обмена	2	
Раздел 2. Угрозы безопасности информационных систем		**6**	
Тема 2.1 Сущность и основные понятие информационной безопасности	**Содержание учебного материала**		ОК 01, ОК 02, ОК 05, ОК 09, ОК 10, ПК11.6
	1 Характеристика составляющих и основные термины и определения информационной безопасности. Основные понятия информационной безопасности в локальных сетях	2	
	Практическое занятие		
	1 Защита информации передаваемой по локальным сетям	2	
Тема 2.2 Основные подходы к классификации угроз информационной безопасности	**Содержание учебного материала**		
	1 Основные подходы к классификации угроз информационной безопасности. Информационные, программно-математические, физические и организационные угрозы	2	
Раздел 3. Защита от несанкционированного доступа, модели и основные принципы защиты информации		**9**	ОК 01, ОК 02, ОК 05, ОК 09, ОК 10, ПК11.6

Тема 3.1 Основные принципы защиты информации от несанкционированного доступа	**Содержание учебного материала**		2	
	1	Модели и основные принципы защиты информации от несанкционированного доступа		
	Практическое занятие		2	
	1	Защита информации от копирования: задание некопируемых меток		
	Самостоятельная работа обучающихся		1	
	1	Защита информации в глобальной сети		
Тема 3.2 Проблемы идентификации и аутентификации пользователей	**Содержание учебного материала**		2	
	1	Проблемы идентификации и аутентификации пользователей. Методы аутентификации и их основные характеристики		
Тема 3.3 Программно-аппаратная защита информации от локального несанкционированного доступа	**Содержание учебного материала**		2	ОК 01, ОК 02, ОК 05, ОК 09, ОК 10, ПК11.6
	1	Программно-аппаратная защита информации от локального несанкционированного доступа. Защита информации от несанкционированного доступа в операционных системах		
Раздел 4. Проблема вирусного заражения программ			**9**	ОК 01, ОК 02, ОК 05, ОК 09, ОК 10, ПК11.6
Тема 4.1 Основные классы антивирусных программ	**Содержание учебного материала**		2	
	1	Структуры современных антивирусных программ. Классификация антивирусных программ		
	Практическое занятие		2	
	1	Инсталляция и настройка антивирусных программ		
Тема 4.2 Методы обнаружения и удаления вирусов	**Содержание учебного материала**		2	
	1	Структура и классификация современных вредоносных программ. Методы обнаружения и удаления вирусов		
	Практическое занятие		2	
	1	Обнаружение современных вредоносных программ		
	Самостоятельная работа обучающихся		1	
	1	Настройка и обновление баз антивирусных программ		
Раздел 5. Защита от утечки информации по техническим каналам			**11**	ОК 01, ОК 02, ОК 05, ОК 09, ОК 10, ПК11.6
Тема 5.1 Прямые и косвенные	**Содержание учебного материала**			

каналы утечки информации.	1	Прямые и косвенные каналы утечки информации. Каналы и методы несанкционированного доступа к конфиденциальной информации	2	
Тема 5.2 Каналы и методы несанкционированного доступа к конфиденциальной информации.	**Содержание учебного материала**			
	1	Понятие канала несанкционированного доступа к защищаемой информации. Классификацию типов каналов несанкционированного доступа к защищаемой информации	2	
Тема 5.3 Обнаружение каналов утечки информации	**Содержание учебного материала**			
	1	Каналы несанкционированного доступа к защищаемой информации с доступом злоумышленника и без доступа злоумышленника. Каналы несанкционированного доступа к защищаемой информации с изменением информации и без изменения информации	2	
Тема 5.4 Методы и средства блокирования каналов утечки информации	**Содержание учебного материала**			
	1	Криптографические средства, обеспечивающие шифрование конфиденциальных данных. Организация доступа к конфиденциальной информации через промежуточные терминальные серверы. Системы активного мониторинга	2	ОК 01, ОК 02, ОК 05, ОК 09, ОК 10, ПК11.6
	Практическое занятие			
	1	Методы шифрование конфиденциальных данных	2	
	Самостоятельная работа обучающихся			
	1	Спецпрограммные комплексы, предназначенные для выявления несанкционированных действий пользователей	1	
Раздел 6. Организационно-правовое обеспечение информационной безопасности			**5**	
Тема 6.1 Служба безопасности объекта. Права и обязанности сотрудников службы безопасности	**Содержание учебного материала**			
	1	Служба безопасности объекта	2	ОК 01, ОК 02, ОК 05, ОК 09, ОК 10, ПК11.6
Тема 6.2 Защита коммерческой тайны и интеллектуальной собственности, основные виды компьютерных преступлений	**Содержание учебного материала**			
	1	Защита коммерческой тайны и интеллектуальной собственности	2	
	Самостоятельная работа обучающихся			
	1	Методы защиты конфиденциальной информации	1	
Промежуточная аттестация			**2**	
Всего:			**48**	

3. УСЛОВИЯ РЕАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

3.1 Требования к минимальному материально-техническому обеспечению

Реализация программы дисциплины требует наличия л**аборатории «Программного обеспечения и сопровождения компьютерных систем»**:

- Автоматизированные рабочие места на 12-15 обучающихся (процессор не ниже Core i3, оперативная память объемом не менее 4 Гб;) или аналоги;
- Автоматизированное рабочее место преподавателя (процессор не ниже Core i3, оперативная память объемом не менее 4 Гб;)или аналоги;
- Проектор и экран;
- Маркерная доска;
- Программное обеспечение общего и профессионального назначения

3.2 Информационное обеспечение обучения

Перечень рекомендуемых учебных изданий, дополнительной литературы

№	Автор	Название	Издательство	Гриф издания	Год издания	Кол-во в библиотеке	Наличие на электронных носителях	Электронные уч. пособия
1	2	3	4	5	6	7	8	9
3.2.1 Основная литература								
3.2.1.1	Партыка Т.Л., Попов И.И.	Информационная безопасность**.** Учебное пособие	Москва: Издательство "ФОРУМ": ООО «Научно-издательский центр ИНФРА-М»		2018		http://znanium.com/go.php?id=915902	
3.2.1.2	Шаньгин В.Ф.	Информационная безопасность**.** Учебное пособие	Москва: Издательство "ФОРУМ": ООО «Научно-издательский центр ИНФРА-М»		2018		http://znanium.com/go.php?id=945331	
3.2.2 Дополнительная литература								
3.2.2.1	Баранова Е.К., Бабаш А.В.	Информационная безопасность и защита информации. Учебное пособие	Москва: Издательский Центр РИОР: ООО "Научно-издательский центр ИНФРА-М"		2018		http://znanium.com/go.php?id=957144	
	Глинская Е.В., Чичварин Н.В.	Информационная безопасность конструкций ЭВМ и систем. Учебное пособие	Москва: ООО "Научно-издательский центр ИНФРА-М"		2018		http://znanium.com/go.php?id=925825	
3.2.3 Периодические издания								
3.2.3.1								
3.2.4 Практические (семинарские) и (или) лабораторные занятия								
3.2.4.1	В.А. Меркулов	Методические указания к выполнению практических работ						
3.2.5 Курсовая работа (проект)								
3.2.5.1								

3.2.6 Контрольные работы								
3.2.6.1								
3.2.7 Программно-информационное обеспечение, Интернет-ресурсы								
3.2.7.1		MS Windows 10 MS Office 2010 Kaspersky Internet Security						

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Контроль и оценка результатов освоения дисциплины осуществляется преподавателем в процессе проведения практических занятий, лекций, домашних контрольных работ, а также выполнения обучающимися индивидуальных практических заданий.

Результаты обучения (освоенные умения, усвоенные знания)	**Формы и методы контроля и оценки результатов обучения**
знать: основные понятия и определения; эволюцию подходов к обеспечению информационной безопасности; информационные, программно-математические, физические и организационные угрозы; структуру современных вирусных программ; основные классы антивирусных программ; перспективные методы антивирусной защиты; организационно-правовое обеспечение информационной безопасности;	тестовый контроль; индивидуальный опрос при проведении занятий; устный ответ у доски; выполнение индивидуальных практических заданий; фронтальный опрос по вариантам; заслушивание сообщений; подготовка докладов; написание рефератов;

уметь: осуществлять защиту от несанкционированного доступа, модели и основные принципы защиты информации; устранять проблемы вирусного заражения программ; организовать защиту от утечки информации по техническим каналам.	домашняя контрольная работа; защита практических работ; составление отчета по проделанной практической работе; составление алгоритма работы; построение блок-схемы.